REMARKS

In the Office Action, the Examiner noted a number of typographical errors in the specification. Applicants submit herein a substitute specification and a markup copy of the substitute specification indicating the changes. With regard to items 1-6, Applicants respectfully submit that the substitute specification includes corrections to the typographical errors noted by the Examiner. With regard to item 7, the Examiner believes that the Applicants have omitted some steps in reaching the conclusions. Applicants respectfully disagree. As stated in lines 1-2 on page 8, the last inequality (equation 4) follows because for any given $m \neq n \in Z_p$ and $\delta \in Z_p$ there is a unique x that satisfies the equation: $m^2 - n^2 + 2(m-n)x = \delta$. Furthermore, as stated in lines 1-2 on page 9 of the specification, the last equation (equation 9) follows because h_x is a universal hash function and $h_x(m)\text{-}h_x(n)$ can take on any value in R with equal probability.

Claims 1-3 are pending in the present application. In the Office Action, claims 1-3 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Examiner's rejections are respectfully traversed.

The Examiner alleges that claims 1-3 only describe a mathematical algorithm without any practical application. Applicants respectfully disagree. Claims 1-3 set forth inputting a collection of bits and then applying the claimed hashing algorithm to the collection of bits to form a hashed collection of bits, $i.e.$, the output modular 2^l result. For example, the claimed method may be used to simplify search for text strings by hashing bits representative of the text strings to reduce the size of the stored information. For another example, the claimed method may be used in various wireless communication applications to shorten authentication messages to a tag. See Patent Application, pages 2-3. Thus, Applicants respectfully submit that the invention set forth in claims 1-3 represents a practical application in the technological arts and is statutory subject

matter. See MPEP §2106 IV.B.2.b.ii. Applicants request that the Examiner's rejections of claims 1-3 under 35 U.S.C. § 101 be withdrawn.

In the Office Action, claims 1-3 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by the Schneier publication. The Examiner's rejections are respectfully traversed.

The Schneier publication describes Jueneman's methods, which teach forming a hash function by applying a mod-p operation, where p is a prime <u>less than 2^m-1</u>. In contrast, claims 1-3 set forth performing a mod-p operation, where p is at least <u>as large as a first prime number greater than 2^n</u>. The Schneier publication also describes an IBC hash, which teaches forming a hash function by applying a mod-p operation to a message M, where p is an n-bit prime number. However, the IBC hash fails to teach or suggest performing a mod-p operation <u>on a squared sum</u>, where p is at least <u>as large as a first prime number greater than 2^n</u>.

For at least the aforementioned reasons, Applicants respectfully submit that the present invention is not anticipated by the Schneier publication and request that the Examiner's rejections of claims 1-3 under 35 U.S.C. § 102(b) be withdrawn.

For the aforementioned reasons, it is respectfully submitted that all claims pending in the present application are in condition for allowance. The Examiner is invited to contact the undersigned at (713) 934-4052 with any questions, comments or suggestions relating to the referenced patent application.

Respectfully submitted,

Date: 1/17/06

Mark W. Sincell, Ph.D.
Reg. No. 52,226
Williams Morgan & Amerson, P.C.
10333 Richmond Avenue, Suite 1100
Houston, TX 77042
(713) 934-7000
(713) 934-7011 (Fax)

AGENT FOR APPLICANTS